

Eisenstein-Dumas criterion and the action of 2×2 nonsingular triangular matrices on polynomials in one variable

Martin Juráš

Key Words and Phrases. *Eisenstein-Dumas criterion, irreducible polynomial, irreducibility criteria, Schönemann-Eisenstein criterion, valued field.*

Abstract Let K be a valued field (in general K is not heselian) with valuation v and $A(x) \in K[x]$ be a polynomial of degree n . We find necessary and sufficient conditions for the existence of the elements $s, t, u \in K$, $s \neq 0 \neq u$, such that at least one of the polynomials $u^n A(\frac{sx+t}{u})$, $(tx+u)^n A(\frac{sx}{tx+u})$, $(ux)^n A(\frac{tx+s}{ux})$ or $(ux+t)^n A(\frac{s}{ux+t})$ is an Eisenstein-Dumas polynomial at v , provided that the characteristic of the residue field of v does not divide n . Furthermore, we show that if the orbit $A(x)GL(2, K)$ contains an Eisenstein-Dumas polynomial at v , then an Eisenstein-Dumas polynomial at v can be found in a certain one-parameter subset of this orbit.

Mathematics Subject Classification (2010): 11R09, 12E05, 12J10.

1 Introduction and results

In the past 150 years, original criteria of Schönemann [8] and Eisenstein [4] were generalized in many different ways. One far reaching generalization comes in the form of a geometric criterion of Dumas [3]:

Newton polygon of a product of polynomials is composed from the sides of polygons of its factors which are ordered with respect to increasing slopes.

In case when the Newton polygon of a polynomial consists of only one line with no interior lattice points, Dumas' criterion implies irreducibility. This special case is called Eisenstein-Dumas criterion:

Let F be a field of fractions of a unique factorization domain R . Let $A(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be a polynomial of degree n and let $p \in R$ be a prime. Denote by v_p the p -adic valuation on F . If

$$(D0) \quad a_0 a_n \neq 0,$$

$$(D1) \quad \gcd(v_p(a_0) - v_p(a_n), n) = 1 \quad \text{and}$$

$$(D2) \quad v_p(a_i) \geq \frac{n-i}{n}v_p(a_0) + \frac{i}{n}v_p(a_n) \quad \text{for } 0 \leq i \leq n,$$

then $A(x)$ is irreducible in $F[x]$.

Below, we present a generalization of this criterion to valued fields (see [2] or [1]). For convenience, we first recall some basic facts about valuations (see, for instance, Jacobson [5] paragraph 9.6).

Let $\Gamma = (\Gamma, +, \leq)$ be a *linearly ordered abelian group*. Let $\infty \notin \Gamma$ and extend the group operation to $\Gamma \cup \{\infty\}$ by $g + \infty = \infty + g = \infty + \infty = \infty$ and set $g < \infty$, for all $g \in \Gamma$. Let K be a field and let K^\times denotes the multiplicative group of K . A function $v : K \rightarrow \Gamma \cup \{\infty\}$ is referred to as *Krull valuation of K* , or *valuation of K* , if it satisfies the following conditions:

- (i) $v(a) = \infty$ iff $a = 0$, for all $a \in K$;
- (ii) $v(ab) = v(a) + v(b)$, for all $a, b \in K$;
- (iii) $v(a + b) \geq \min\{v(a), v(b)\}$, for all $a, b \in K$.

A field endowed with a valuation is called a *valued field*.

The ring $R_v = \{a \in K : v(a) \geq 0\}$ is called the *valuation ring of v* . The ideal $M_v = \{a \in K : v(a) > 0\}$ is called the *prime ideal of v* or the *maximal ideal of v* . The field $K_v = R_v/M_v$ is called the *residue field of v* . Any valuation v satisfies these basic properties: $v(1) = v(-1) = 0$, $v(a^{-1}) = -v(a)$ for all $a \in K^\times$, and $v(a + b) = \min\{v(a), v(b)\}$ provided $v(a) \neq v(b)$.

Throughout this paper, K denotes a valued field with value group Γ and a non-trivial valuation $v : K \rightarrow \Gamma \cup \{\infty\}$. K is not assumed to be henselian, unless specifically stated.

Theorem 1.1 is a special case of a result by Brown (cf. [2], Lemma 4).

Theorem 1.1. [Eisenstein-Dumas criterion] Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . If

$$(D0) \quad a_n a_0 \neq 0;$$

$$(D1) \quad v(a_0) - v(a_n) \notin k\Gamma = \{kg : g \in \Gamma\} \text{ for any integer } k > 1 \text{ that divides } n;$$

$$(D2) \quad nv(a_i) \geq (n-i)v(a_0) + iv(a_n) \quad \text{for } 0 \leq i \leq n;$$

then $A(x)$ is irreducible in $K[x]$.

A polynomial satisfying conditions (D0), (D1) and (D2) of Theorem 1.1 is referred to as *Eisenstein-Dumas polynomial (at v)*.

Classical invariant theory studies intrinsic properties of binary homogeneous forms $A(x, y) = \sum_{i=0}^n a_i x^i y^{n-i}$, $a_i \in K$, with regards to the right action of $GL(2, K)$:

$$A(x, y)g = \sum_{i=0}^n a_i (ax + by)^i (cx + dy)^{n-i} \quad \text{for } g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, K).$$

Each binary form of degree n , corresponds to the (inhomogeneous) polynomial $A(x) = A(x, 1)$. Conversely, given a polynomial $A(x)$, we can recover its homogeneous form by the rule $A(x, y) = y^n A(\frac{x}{y})$, provided we a priori specify the degree n . The degree of a non-trivial binary form is the degree of any of its monomials. *The degree of a polynomial $A(x)$ is equal to the degree of the homogeneous form corresponding to $A(x)$* (cf., for instance, [7], Chapter 2).

The action of $GL(2, K)$ on $K[x]$ is given by the linear fraction transformation:

$$A(x)g = (cx + d)^n A\left(\frac{ax + b}{cx + d}\right) \quad \text{for } A(x) \in K[x], \quad g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, K),$$

where n is the degree of $A(x)$.

The definition of the degree above guarantees that *all polynomials in the orbit $A(x)GL(2, K)$ have the same degree*. For instance, consider the 3rd-degree polynomial $A(x) = x^3 + x^2 - 2$, which corresponds to the form $A(x, y) = x^3 + x^2y - 2y^3$. Then, $B(x) = A(x) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = -5x^2 - 6x - 2$ is a polynomial of degree 3, corresponding to the binary form $B(x, y) = -5x^2y - 6xy^2 - 2y^3$.

Given a polynomial $A(x) \in K[x]$ of degree n , we are interested in finding criteria which ensure that the orbit $A(x)GL(2, K)$ contains an Eisenstein-Dumas polynomial.

In this paper we obtained some partial results.

Note that all irreducible polynomials cannot be found by application Eisenstein-Dumas criterion and the action of $GL(2, K)$. For example, $A(x) = x^4 - 14x^2 + 9$ is irreducible in $\mathbb{Q}[x]$, but the orbit $A(x)GL(2, \mathbb{Q})$ contains no Eisenstein-Dumas polynomial at any valuation v of \mathbb{Q} (cf. [6], page 229).

In [6], Theorem 2.3, we proved:

Let F be a field of fractions of a unique factorization domain R . Let $A(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be a polynomial of degree n and let $p \in R$ be a prime. Assume that the characteristic of R does not divide n and p does not divide $n1_R$. If there are $s, t \in F$, $s \neq 0$ such that $A(sx + t)$ is an Eisenstein-Dumas polynomial at v_p , then $A(x - \frac{a_{n-1}}{na_n})$ is an Eisenstein-Dumas polynomial at the p -adic valuation v_p .

A straightforward application of this last theorem yields the irreducibility, in $\mathbb{Q}[x]$, of the p -th cyclotomic polynomial $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ (for an odd prime p); by simple divisibility arguments, one can show that $\Phi_p(x - \frac{1}{p-1})$ is an Eisenstein polynomial at v_p . Notice that the transformation suggested by the theorem, $x \mapsto x - \frac{1}{p-1}$, is not the usual one $x \mapsto x + 1$. But, $-\frac{1}{p-1} = 1$ in $GF(p)$, and the two transformations are connected by means of Lemma 2.3, since $\Phi_p(x - \frac{1}{p-1}) = \Phi_p(x + 1 - \frac{p}{p-1})$ and $v(-\frac{p}{p-1}) = 1 > \frac{1}{p-1}$.

Bishnoi and Khanduja generalized [6], Theorem 2.3, to henselian valued fields ([1], Theorem 1.2):

Let $g(x) = \sum_{i=1}^e a_i x^i$ be a monic polynomial with coefficients in a henselian field (K, v) . Suppose that the characteristic of the residue field of v does not divide e . If there exists an element $b \in K$ such that $g(x + b)$ is an Eisenstein-Dumas polynomial with respect to v , then so is $g(x - \frac{a_{e-1}}{e})$.

The next result generalizes the theorem above.

Theorem 1.2. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If, for some element $g = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in GL(2, K)$ with $stuv = 0$, $A(x)g$ is an Eisenstein-Dumas polynomial, then at least one of the two polynomials

$$U(A(x)) = A(x) \begin{bmatrix} 1 & -\frac{a_{n-1}}{na_n} \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad L(A(x)) = A(x) \begin{bmatrix} 1 & 0 \\ -\frac{a_1}{na_0} & 1 \end{bmatrix}$$

is an Eisenstein-Dumas polynomial.

In the proof of [1], Theorem 1.2, Bishnoi and Khanduja utilized ramification theory of algebraic field extensions and used the fact that the field K is henselian. Theorem 1.2 applies to *any* valued field K ; our proof is a modification of the author's proof of [6], Theorem 2.3.

Let $A(x) \in \mathbb{Q}[x]$ be a polynomial of degree n . Theorem 1.2 implies that there are at most finitely many prime numbers $p \in \mathbb{Z}$, for which there is $g = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in GL(2, \mathbb{Q})$, $stuv = 0$, such that $A(x)g$ is an Eisenstein-Dumas polynomial at some p -adic valuation v_p . Indeed, for such a p , if b_0 and b_n denote the constant coefficient and the leading coefficient of $U(A(x))$, and c_0 and c_n denote the constant coefficient and the leading coefficient of $L(A(x))$, then, due to (D1), p satisfies at least one of the three conditions below: (i) $\gcd(v_p(\frac{b_0}{b_n}), n) = 1$ or (ii) $\gcd(v_p(\frac{c_0}{c_n}), n) = 1$ or (iii) p divides n .

Theorem 1.3. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . If one of the two polynomials $U(A(x))$ or $L(A(x))$ is an Eisenstein-Dumas polynomial, then $A(x)$ is irreducible.

Theorem 1.3 follows immediately from Theorem 1.1 and the fact that the incredibility of $A(x)$ is invariant under the action of $GL(2, K)$. Due to Theorem 1.2, one may expect Theorem 1.3 to be more useful in establishing irreducibility of polynomials than Theorem 1.1. There are instances though, when Theorem 1.1 applies and Theorem 1.3 fails. This may occur when the characteristic of the residue field of v divides the degree of $A(x)$. For example, consider $A(x) = x^2 + 4x + 8 \in \mathbb{Q}[x]$, which is an Eisenstein-Dumas polynomial at the 2-adic valuation v_2 , but neither $U(A(x)) = x^2 + 4$ nor $L(A(x)) = \frac{1}{2}x^2 + 8$ is an Eisenstein-Dumas polynomial.¹

¹Condition (D1) of Theorem 1.1 fails in both cases.

Proposition 1.4. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n and let $B(x) = \sum_{i=0}^n a_{n-i} x^i$. Then

$$U(B(x)) = L(A(x)) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Furthermore, $L(A(x))$ is an Eisenstein-Dumas polynomial iff $U(B(x))$ is an Eisenstein-Dumas polynomial.

Theorem 1.5. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If the orbit $A(x)GL(2, K)$ contains an Eisenstein-Dumas polynomial, then one of the two polynomials $U(A(x))$ or $L(A(x))$ is an Eisenstein-Dumas polynomial or there is $t \in K$ such that $A'(t) \neq 0$ and the polynomial

$$A(x) \begin{bmatrix} t & \phi(t) \\ 1 & 1 \end{bmatrix} = (x+1)^n A\left(\frac{tx+\phi(t)}{x+1}\right), \quad \text{where } \phi(t) = t - n \frac{A(t)}{A'(t)},$$

is an Eisenstein-Dumas polynomial. (A' is the derivative of A .)

This last result generalizes [6], Theorem 3.2.

2 Proofs

Theorem 1.1 not only generalizes numerous versions of Schönemann-Eisenstein criterion, but also exhibits symmetries of the irreducibility conditions that are absent under the conditions of the primer criteria of Schönemann [8] and Eisenstein [4]. There are two obvious families of symmetries generated by group actions of K^\times and a discrete symmetry. The proof of the following lemma is straightforward.

Lemma 2.1. Let $A(x) \in K[x]$ and $t \in K^\times$. Then

(i) $tA(x)$ is an Eisenstein-Dumas polynomial iff $A(x)$ is an Eisenstein-Dumas polynomial.

(ii) $A(tx) = A(x) \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}$ is an Eisenstein-Dumas polynomial iff $A(x)$ is an Eisenstein-Dumas polynomial.

(iii) $x^n A(\frac{1}{x}) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is an Eisenstein-Dumas polynomial iff $A(x)$ is an Eisenstein-Dumas polynomial.

Lemma 2.2. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Then the conditions (D0), (D1), (D2) in Theorem 1.1 are equivalent to (D0), (D1), (D2'), where

(D2') $nv(a_i) > (n-i)v(a_0) + iv(a_n)$ for $1 \leq i \leq n-1$.

Proof. (D2) is always trivially satisfied for $i = 0$ and $i = n$ and so (D0),(D1),(D2') implies (D0),(D1),(D2). Let (D0),(D1), (D2) hold and assume, by contraposition, that $nv(a_i) = (n - i)v(a_0) + iv(a_n)$, for some i , $1 \leq i \leq n - 1$. Then $ig = nh$ where $g = v(a_0) - v(a_n)$ and $h = v(a_0) - v(a_i)$. Let $c = \gcd(i, n)$. Obviously, $c < n$. There are $a, b \in \mathbb{Z}$ such that $ai + bn = c$. Multiplying the last equation by $\frac{g}{c}$ and using $ig = nh$ we arrive at $\frac{n}{c}(ah + bg) = g$. $\frac{n}{c}$ is an integer greater than 1 which divides n and $ah + bg \in \Gamma$. The last equation contradicts (D1). \blacksquare

Lemma 2.3. *Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be an Eisenstein-Dumas polynomial of degree n . Assume that $t \in K$, $nv(t) > v(a_0) - v(a_n)$. Then*

$$A(x) \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} = A(x + t)$$

is an Eisenstein-Dumas polynomial.

Proof. $\bar{A}(x) = \sum_{i=0}^n \bar{a}_i x^i = A(x + t)$, where

$$\bar{a}_i = \sum_{k=i}^n \binom{k}{i} a_k t^{k-i} \quad \text{for all } 0 \leq i \leq n.$$

In particular, $\bar{a}_n = a_n \neq 0$, and so $v(\bar{a}_n) = v(a_n)$, and $\bar{a}_0 = A(t)$. If $\bar{a}_0 = 0$, then t is a root of $A(x)$, a contradiction. Thus $\bar{a}_0 \neq 0$ and so (D0) is satisfied for $\bar{A}(x)$.

For $0 < k \leq n$, we have

$$\begin{aligned} nv(a_k t^k) &= n[v(a_k) + kv(t)] \geq (n - k)v(a_0) + kv(a_n) + knv(t) \\ &> (n - k)v(a_0) + kv(a_n) + k(v(a_0) - v(a_n)) = nv(a_0). \end{aligned}$$

Hence, $v(a_k t^k) > v(a_0)$ for $0 < k \leq n$. Since, $\bar{a}_0 = a_0 + \sum_{k=1}^n a_k t^k$, then $v(\bar{a}_0) = v(a_0)$ and so (D1) holds for $\bar{A}(x)$.

We now show that (D2) is satisfied for $\bar{A}(x)$. For $i \leq k$, we have

$$\begin{aligned} nv\left(\binom{k}{i} a_k t^{k-i}\right) &\geq n[v(a_k) + (k - i)v(t)] \geq (n - k)v(a_0) + kv(a_n) \\ &+ (k - i)(v(a_0) - v(a_n)) = (n - i)v(a_0) + iv(a_n) = (n - i)v(\bar{a}_0) + iv(\bar{a}_n) \end{aligned}$$

Thus, for $0 \leq i \leq n$,

$$nv(\bar{a}_i) = nv\left(\sum_{k=i}^n \binom{k}{i} a_k t^{k-i}\right) \geq (n - i)v(\bar{a}_0) + iv(\bar{a}_n).$$

\blacksquare

To prove the following lemma, we need $v(n1) = 0$. Bishnoi and Khanduja (see [1], Theorem 1.2) found an elegant equivalent condition, namely that the characteristic of the residue field of v does not divide n .

Lemma 2.4. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If $A(x)$ is an Eisenstein-Dumas polynomial, then $nv(\frac{a_{n-1}}{na_n}) > v(a_0) - v(a_n)$.

Proof. First we use the fact that the characteristic of the residue field of v , K_v , does not divide n to show that $v(n1) = 0$.

Assume, by contraposition, that $v(n1) \neq 0$. Since $v(1) = 0$, it follows $v(n1) > 0$, and so $n1 \in M_v$. Hence, $n\varphi(1) = \varphi(n1) = 0$, where $\varphi : R_v \rightarrow R_v/M_v$ is the canonical homomorphism. Thus, the characteristic of K_v divides n , which yields a contradiction.

Since $n1 \neq 0$, then $na_n = (n1)a_n \neq 0$.

Furthermore, assume that $A(x)$ is an Eisenstein-Dumas polynomial. Using (D2') in Lemma 2.2 with $i = n - 1$, we obtain

$$\begin{aligned} nv\left(\frac{a_{n-1}}{na_n}\right) &= n[v(a_{n-1}) - v(a_n) - v(n1)] \\ &> v(a_0) + (n - 1)v(a_n) - nv(a_n) = v(a_0) - v(a_n). \end{aligned}$$

■

Proof of Theorem 1.2

Theorem 1.2 will be established by proving Theorems 2.5 – 2.8. Each of these theorems will deal with a partial case of Theorem 1.2.

By $U(2, K)$, resp., $L(2, K)$ we denote the multiplicative group of all upper, resp., lower triangular matrices in $GL(2, K)$.

Theorem 2.5. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If the orbit $A(x)U(2, K)$ contains an Eisenstein-Dumas polynomial, then

$$U(A(x)) = A(x) \begin{bmatrix} 1 & -\frac{a_{n-1}}{na_n} \\ 0 & 1 \end{bmatrix} = A\left(x - \frac{a_{n-1}}{na_n}\right) \quad (1)$$

is an Eisenstein-Dumas polynomial.

Proof. Let $g = \begin{bmatrix} s & t \\ 0 & u \end{bmatrix} \in U(2, K)$ and assume that

$$\bar{A}(x) = \sum_{i=0}^n \bar{a}_i x^i = A(x)g = u^n A\left(\frac{sx+t}{u}\right)$$

is an Eisenstein-Dumas polynomial.

By Lemma 2.4, $nv(\frac{\bar{a}_{n-1}}{n\bar{a}_n}) > v(\bar{a}_0) - v(\bar{a}_n)$ and by Lemma 2.3,

$$B(x) = \bar{A}(x) \begin{bmatrix} 1 & -\frac{\bar{a}_{n-1}}{n\bar{a}_n} \\ 0 & 1 \end{bmatrix}$$

is an Eisenstein-Dumas polynomial. By Lemma 2.1(i,ii), $(\frac{1}{u})^n B(\frac{u}{s}x)$ is an Eisenstein-Dumas polynomial. Using $0 \neq \bar{a}_n = a_n s^n$ and $\bar{a}_{n-1} = s^{n-1}(na_n t + a_{n-1}u)$, we obtain

$$\begin{aligned} (\frac{1}{u})^n B(\frac{u}{s}x) &= B(x) \begin{bmatrix} \frac{1}{s} & 0 \\ 0 & \frac{1}{u} \end{bmatrix} = \bar{A}(x) \begin{bmatrix} 1 & -\frac{\bar{a}_{n-1}}{n\bar{a}_n} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{s} & 0 \\ 0 & \frac{1}{u} \end{bmatrix} \\ &= A(x) \begin{bmatrix} s & t \\ 0 & u \end{bmatrix} \begin{bmatrix} 1 & -\frac{t}{s} - \frac{a_{n-1}u}{na_n s} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{s} & 0 \\ 0 & \frac{1}{u} \end{bmatrix} = A(x) \begin{bmatrix} 1 & -\frac{a_{n-1}}{na_n} \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

■

Theorem 2.6. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If the orbit $A(x)L(2, K)$ contains an Eisenstein-Dumas polynomial, then

$$L(A(x)) = A(x) \begin{bmatrix} 1 & 0 \\ -\frac{a_1}{na_0} & 1 \end{bmatrix} = (1 - \frac{a_1}{na_0}x)^n A\left(\frac{x}{1 - \frac{a_1}{na_0}x}\right) \quad (2)$$

is an Eisenstein-Dumas polynomial.

Proof. Let $g = \begin{bmatrix} s & 0 \\ t & u \end{bmatrix} \in L(2, K)$. Assume that $\bar{A}(x) = A(x)g$ is an Eisenstein-Dumas polynomial. By Lemma 2.1(iii), $x^n \bar{A}(\frac{1}{x})$ is also an Eisenstein-Dumas polynomial. We have

$$\begin{aligned} x^n \bar{A}(\frac{1}{x}) &= \bar{A}(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} s & 0 \\ t & u \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &= A(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u & t \\ 0 & s \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = B(x) \begin{bmatrix} u & t \\ 0 & s \end{bmatrix} \end{aligned}$$

where $B(x) = A(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \sum_{i=0}^n a_{n-i} x^i$. Since $\begin{bmatrix} u & t \\ 0 & s \end{bmatrix} \in U(2, K)$, then by Theorem 2.5, $B(x) \begin{bmatrix} 1 & -\frac{a_1}{na_0} \\ 0 & 1 \end{bmatrix}$ is an Eisenstein-Dumas polynomial.

$$B(x) \begin{bmatrix} 1 & -\frac{a_1}{na_0} \\ 0 & 1 \end{bmatrix} = A(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -\frac{a_1}{na_0} \\ 0 & 1 \end{bmatrix} = A(x) \begin{bmatrix} 0 & 1 \\ 1 & -\frac{a_1}{na_0} \end{bmatrix}$$

By Lemma 2.1(iii)

$$A(x) \begin{bmatrix} 0 & 1 \\ 1 & -\frac{a_1}{na_0} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} 1 & 0 \\ -\frac{a_1}{na_0} & 1 \end{bmatrix} = L(A(x))$$

is an Eisenstein-Dumas polynomial. ■

Theorem 2.7. Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If the orbit, $A(x)U(2, K) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ contains an Eisenstein-Dumas polynomial, then the polynomial $U(A(x))$ is an Eisenstein-Dumas polynomial.

Proof. Let $g = \begin{bmatrix} t & s \\ u & 0 \end{bmatrix} \in U(2, K) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ be such that $B(x) = A(x)g = (ux)^n A\left(\frac{tx+s}{ux}\right)$ is an Eisenstein-Dumas polynomial.

By Lemma 2.1(iii), $x^n B\left(\frac{1}{x}\right)$ is an Eisenstein-Dumas polynomial. We have

$$x^n B\left(\frac{1}{x}\right) = B(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} t & s \\ u & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} s & t \\ 0 & u \end{bmatrix}$$

Since $\begin{bmatrix} s & t \\ 0 & u \end{bmatrix} \in U(2, K)$, the statement follows from Theorem 2.5. \blacksquare

Theorem 2.8. *Let $A(x) = \sum_{i=0}^n a_i x^i \in K[x]$ be a polynomial of degree n . Assume that the characteristic of the residue field of v does not divide n . If the orbit $A(x)L(2, K) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ contains an Eisenstein-Dumas polynomial, then the polynomial $L(A(x))$ is an Eisenstein-Dumas polynomial.*

Proof. Let $g = \begin{bmatrix} 0 & s \\ u & t \end{bmatrix} \in L(2, K) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ be such that $B(x) = A(x)g = (ux + t)^n A\left(\frac{s}{ux+t}\right)$ is an Eisenstein-Dumas polynomial. By Lemma 2.1 (iii), $x^n B\left(\frac{1}{x}\right)$ is an Eisenstein-Dumas polynomial of degree n . We have

$$x^n B\left(\frac{1}{x}\right) = B(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} 0 & s \\ u & t \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A(x) \begin{bmatrix} s & 0 \\ t & u \end{bmatrix}$$

Since $\begin{bmatrix} s & 0 \\ t & u \end{bmatrix} \in L(2, K)$, the statement now follows from Theorem 2.6. \blacksquare

This completes the proof of Theorem 1.2.

Proof of Proposition 1.4

Proof. We have

$$\begin{aligned} U(B(x)) &= B(x) \begin{bmatrix} 1 & -\frac{a_1}{na_0} \\ 0 & 1 \end{bmatrix} = A(x) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -\frac{a_1}{na_0} \\ 0 & 1 \end{bmatrix} \\ &= A(x) \begin{bmatrix} 0 & 1 \\ 1 & -\frac{a_1}{na_0} \end{bmatrix} = A(x) \begin{bmatrix} 1 & 0 \\ -\frac{a_1}{na_0} & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = L(A(x)) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \end{aligned}$$

The last sentence now follows from Lemma 2.1(iii). \blacksquare

Proof of Theorem 1.5

Proof. Let $\begin{bmatrix} s & t \\ u & v \end{bmatrix} \in GL(2, K)$ and assume $\bar{A}(x) = A(x)g$ is an Eisenstein-Dumas polynomial. If $stuv = 0$, then by Theorem 1.2, one of the two polynomials $U(A(x))$ or $L(A(x))$ is an Eisenstein-Dumas polynomial.

Assume that $stuv \neq 0$. By Lemma 2.1(i,ii), $B(x) = \sum_{i=1}^n b_i x^i = (\frac{1}{v})^n \bar{A}(\frac{v}{u}x)$ is an Eisenstein-Dumas.

$$B(x) = \bar{A}(x) \begin{bmatrix} \frac{1}{u} & 0 \\ 0 & \frac{1}{v} \end{bmatrix} = A(x) \begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} \frac{1}{u} & 0 \\ 0 & \frac{1}{v} \end{bmatrix} = A(x) \begin{bmatrix} \frac{s}{u} & \frac{t}{v} \\ 1 & 1 \end{bmatrix}.$$

By Lemma 2.4, $nv(\frac{b_{n-1}}{nb_n}) > v(b_0) - v(b_n)$. By Lemma 2.3,

$$\bar{B}(x) = B(x) \begin{bmatrix} 1 & -\frac{b_{n-1}}{nb_n} \\ 0 & 1 \end{bmatrix} = B(x - \frac{b_{n-1}}{nb_n})$$

is an Eisenstein-Dumas polynomial. Moreover,

$$b_n = A(e) \quad \text{and} \quad b_{n-1} = (f - e) A'(e) + n A(e),$$

where $e = \frac{s}{u}$ and $f = \frac{t}{v}$. $A(e) = b_n \neq 0$ since $B(x)$ is of degree n .

If $A'(e) = 0$, then

$$\bar{B}(x) = A(x) \begin{bmatrix} e & f \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = A(x) \begin{bmatrix} e & f - e \\ 1 & 0 \end{bmatrix},$$

and so by Theorem 2.7, $U(A(x))$ is an Eisenstein-Dumas polynomial.

Assume that $A'(e) \neq 0$. Then, by Lemma 2.1(i,ii),

$$C(x) = \left(\frac{nA(e)}{(e-f)A'(e)} \right)^n \bar{B} \left(\frac{(e-f)A'(e)}{nA(e)} x \right)$$

is an Eisenstein-Dumas polynomial. We have

$$\begin{aligned} C(x) &= \bar{B}(x) \begin{bmatrix} 1 & 0 \\ 0 & \frac{nA(e)}{(e-f)A'(e)} \end{bmatrix} \\ &= B(x) \begin{bmatrix} 1 & \frac{(f-e)A'(e)+nA(e)}{nA(e)} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{nA(e)}{(e-f)A'(e)} \end{bmatrix} \\ &= A(x) \begin{bmatrix} e & f \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{(f-e)A'(e)+nA(e)}{nA(e)} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{nA(e)}{(e-f)A'(e)} \end{bmatrix} \\ &= A(x) \begin{bmatrix} e & e - n \frac{A(e)}{A'(e)} \\ 1 & 1 \end{bmatrix} \end{aligned}$$

■

References

- [1] A. Bishnoi and S. K. Khanduja, *On Eisenstein-Dumas and Generalized Schönenmann polynomials*, Comm. Algebra **38**(2010), pp. 3163-3173.

- [2] Brown, R., *Roots of generalized Schönemann polynomials in henselian extension fields*, Indian J. Pure Appl. Math. **39**(5)(2008), pp. 403–410.
- [3] G. Dumas, *Sur quelques cas d’irréductibilité des polynômes à coefficients rationnels*, Journal de math. Pures et Appliqués Soc. **2** (1906), pp. 191–258.
- [4] G. Eisenstein, *Über die Irreduzibilität und einige andere Eigenschaften der Gleichungen*, Journal für die Mathematik **39**(1850), pp. 160–179.
- [5] H. Jacobson, Basic algebra II (2nd ed.), Dover Books on Mathematics, Paperback, 2009.
- [6] M. Juráš, *Eisenstein-Dumas criterion for irreducibility of polynomials and projective transformations of the independent variable*, JP Jour. Algebra, Number Theory, and Appl. **6**(2) (2006), pp. 221–236.
- [7] P. J. Olver, Classical invariant theory, London Mathematical Society Student Texts **44**, Cambridge University Press, 1999.
- [8] T. Schönemann, *Von denjenigen moduln, welche potenzen von primzahlen sind*, Journal für die Reine und Angew. Math. **32** (1846), pp. 93–105.